The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A malware detection system for determining whether a code module is malware according to the code module's exhibited behaviors, the system comprising:

at least one dynamic behavior evaluation module, wherein each dynamic behavior evaluation module provides a virtual environment in which a code module of a particular type may be executed, and wherein each dynamic behavior evaluation module records some behaviors which may be exhibited by the code module as it is executed into a behavior signature;

a management module for obtaining the code module and selecting a dynamic behavior evaluation module to execute the code module according to the code module's type;

a malware behavior signature store storing at least one known malware behavior signature; and

a behavior signature comparison module that obtains the behavior signature and compares the behavior signature to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited behaviors of the code module match the exhibited behaviors of known malware.

2. A malware detection system for determining whether a code module is malware according to the code module's exhibited behaviors, the system comprising:

at least one behavior evaluation means, wherein each behavior evaluation means provides a virtual environment in which a code module of a particular type may be executed, and wherein each behavior evaluation means records some behaviors which may be exhibited by the code module as it is executed into a behavior signature;

a management means for obtaining the code module and selecting a behavior evaluation means to execute the code module according to the code module's type;

a storage means for storing at least one known malware behavior signature; and

a behavior comparison means for comparing the behavior signature to the known malware behavior signatures in the storage means to determine whether the exhibited behaviors of the code module match the exhibited behaviors of known malware.

3. A method for determining whether a code module is malware according to the code module's exhibited behaviors, the method comprising:

selecting a dynamic behavior evaluation module according to the executable type of the code module;

executing the code module in the selected dynamic behavior evaluation module, wherein the selected dynamic behavior evaluation module provides a virtual environment in which the code module may be safely executed;

recording some behaviors exhibited by the code module executing in the dynamic behavior evaluation module;

comparing the recorded behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware behaviors; and

according to the results of the previous comparison, determining whether the code module is malware.

4. A computer-readable medium bearing computer-executable instructions which, when executed, carry out a method for determining whether an executable code module is malware according to the code module's exhibited behaviors, the method comprising:

selecting a dynamic behavior evaluation module according to the executable type of the code module;

executing the code module in the selected dynamic behavior evaluation module, wherein the selected dynamic behavior evaluation module provides a virtual environment in which the code module may be safely executed;

recording some behaviors exhibited by the code module executing in the dynamic behavior evaluation module;

comparing the recorded behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware behaviors; and

according to the results of the previous comparison, determining whether the code module is malware.